**DEPARTMENT OF THE NAVY**
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

SECNAVINST 3501.1
DON CIO
16 June 2002

SECNAV INSTRUCTION 3501.

From: Secretary of the Navy

Subj: DEPARTMENT OF NAVY (DON) CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Ref: (a) Presidential Decision Directive/ NSC 63, "Critical Infrastructure Protection", of 22 May 98
(b) Department of Defense Critical Infrastructure Protection (CIP) Plan, 18 Nov 98

Encl: (1) Critical Infrastructure Definitions
(2) Department of the Navy Critical Infrastructure Planning Council
(3) Department of the Navy Critical Infrastructure Working Group

1. Purpose. To delineate Department of the Navy (DON) policy and responsibilities for implementing Critical Infrastructure Protection (CIP).

2. Scope. This directive applies to the Offices of the Secretary of the Navy, the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all Navy and Marine Corps activities, installations, commands, units, and personnel.

3. Definitions. Accepted CIP terminology is provided in enclosure (1).

4. Background. Reference (a) outlines our national intent to identify and protect our critical infrastructures. Reference (b) is the Department of Defense (DoD) plan for protection of the Defense Infrastructure (DI).

The Under Secretary of the Navy, by a 26 August 1999 memorandum, "…in order to provide a comprehensive approach to protecting the Department's critical infrastructures…" appointed the DON Chief Information Officer (CIO) the DON Critical Infrastructure Assurance Officer (CIAO). Because "Protection of both our physical and cyber infrastructures is an enormous task that will require the active collaboration and participation of

organizations throughout our enterprise…," the memorandum further established the DON Critical Infrastructure Protection (CIP) Council (enclosure (2)), and prompted the creation of a DON CIP Working Group (enclosure (3)) to directly relate to the DOD CIP organization created by reference (b). The tasking of these new entities was "…to meet the requirements of the National Plan for Information Systems Protection, the Critical Infrastructure Protection Plan, the Critical Asset Assurance Program, and the Defense-wide Information Assurance Program."

5. Discussion. DoD/DON CIP is oriented to complement and ensure warfighter mission assurance. It encourages participation by all hands to identify possible vulnerabilities, defend against their possible exploitation, and if exploited, minimize the impact to mission completion. CIP not only encompasses traditional aspects of security (Anti-Terrorism/Force Protection, Operational Security, Physical Security, Information and Infrastructure Assurance), but also shall be considered a critical element in acquisition and operations planning which supports overall mission assurance by linking assets to DON operations. There are six life cycle phases – Infrastructure Analysis and Assessment, Remediation, Indications and Warning, Mitigation, Response, and Reconstitution – that span activities that occur before, during, and after events, which may result in infrastructure compromise or disruption. A key aspect of CIP is recognizing the importance of DON assets and installations in supporting Regional Commander and Commander-in-Chief (CINC) requirements, particularly CINC Operations Plans (OPLANs). Paragraph 4.8 of reference (b) notes the unique place installations occupy in the CIP structure, as they are the primary interface with host nation, federal, state, and local protection activities.

6. Policy. It is DON policy to:

a. Protect infrastructures deemed critical to DON force and materiel readiness and operations in peace, crisis, and war; mitigate the effect of their loss or disruption; and/or plan for timely restoration or recovery.

b. Recognize that DON equipment, facilities, utilities, services, weapon systems, and mission accomplishment are highly dependent upon non-DON assets, including national/international

infrastructures, facilities and services of the private sector, and other government departments and agencies. That these non-DON assets are often essential to the functioning of DON assets is cause for concern and requires special attention.

c. Observe, report, and propose administrative action required in the protection of non-DON infrastructures and assets whose security is primarily with the private and non-military asset owners and with local, State, and Federal law enforcement authorities; including non-United States infrastructures and assets that are the responsibility of appropriate foreign and national authorities for protecting.

d. Increase the awareness of the CIP program through information sharing, cooperative agreements and outreach with the private sector, education partnerships, State and local government partnerships, exchange of personnel, training and education, and other efforts.

e. Determine the risk to mission-critical systems and processes supporting logistics and acquisition. Non-organic infrastructures and services that serve as sole source producers/single nodes of vulnerability in delivery and operational sustainment of Acquisition Category I through IV weapons systems, or any other critical acquisition programs, shall be considered. Acquisition management procedures shall be modified as necessary to achieve weapon system mission assurance.

f. Use the results of the various analyses performed under the CIP program, such as the risk analysis and business impact analysis, to determine needed funding, and to obtain management approval of resources and actions for effectuating changes in business practices or procedures to protect critical infrastructures/assets.

7. Action

a. The Department of the Navy Chief Information Officer (DON CIO) shall serve as the Department of the Navy Critical Infrastructure Assurance Officer (DON CIAO) and shall:

(1) Represent the DON on the DOD CIAO Council and

provide membership to the DOD Critical Infrastructure Protection Implementation Staff (CIPIS).

(2) Oversee DON CIP initiatives and coordinate activities with the Secretariat, CNO and CMC as appropriate;

(3) Chair the DON Critical Infrastructure Protection Council and conduct meetings as needed;

(4) Serve as the central point of contact for CIP-related issues, to include establishing and maintaining a secure database of Tier I and II assets, remediation efforts, programmatic and budgetary expenditures for CIP, DON personnel points of contact, and liaison with other existing CIP-related security programs.

(5) Assign staff member(s) to coordinate the actions of the DON CIP Working Group.

(6) Develop information-sharing strategies for CIP initiatives.

(7) Develop new, or leverage existing, CIP self-assessment tools and provide them to asset owners.

(8) Coordinate the identification and notification of DON Tier I and II assets.

(9) Sponsor and provide oversight for a new Naval Integrated Vulnerability Assessment (NIVA) program closely coordinated with the existing CNO (N34) and CMC (Code POS) Integrated Vulnerability Assessment (IVA) processes; computer network defense assessment capabilities resident in Fleet Information Warfare Center (FIWC) and Marine Information Technology and Network Operations Center (MITNOC); non-organic and organic mission infrastructure dependencies analysis and assessment expertise resident at Joint Program Office–Special Technology Countermeasures (JPO-STC); disaster preparedness and continuity of operations plans assessments and reviews; and other mission-focused critical infrastructure assessment protocols yet to be identified or defined.

(10) Ensure that DON CIP efforts support and are integrated with DOD/Joint CIP initiatives.

b. The Assistant Secretary of the Navy, (Research, Development and Acquisition) (ASN(RD&A)) shall:

(1) Serve as a member of the DON CIP Council;

(2) Provide the Acquisition Community member to the DON CIP Working Group, who will also serve as the DON representative to the USD (AT&L)-led Office of the Secretary of Defense (OSD) CIP Industrial Sector Working Group;

(3) Work with the DON CIAO to identify, characterize, prioritize, and remediate vulnerabilities to critical non-organic infrastructures and processes managed by the acquisition community;

(4) Review policies that may be affected by CIP consideration and revise as necessary; and

(5) Require CIP consideration in contracts for weapon systems and their contractor provided support.

c. The Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN(FM&C)) shall:

(1) Serve as a member of the DON CIP Council;

(2) Provide the Financial Sector member to the DON CIP Working Group, who will also serve as the DON representative to the DFAS-led OSD CIP Financial Sector Working Group;

(3) Identify and rank critical, DON owned and managed, financial infrastructures;

(4) Participate in the conduct of vulnerability assessments of DON critical financial infrastructures and develop CIP sensitive procedures for remediation, mitigation, and assurance that the minimum essential level of financial operations can be protected and maintained; and

(5) Work with the other CIP sectors, as required, in addressing security requirements of DON financial infrastructures.

d. The Assistant Secretary of the Navy (Installations and Environment) (ASN(I&E)) shall:

(1) Serve as a member of the DON CIP Council;

(2) Provide the Public Works Sector lead(s) to the DON CIP Working Group who will also serve as the DON representative to the U.S. Army Corps of Engineers-led OSD CIP Public Works Sector Working Group;

(3) Make CIP an integral factor in policies directing facilities and utilities planning, design, construction, and maintenance; and

(4) Thoroughly integrate CIP in plans and policies implementing utilities privatization, strategic sourcing, Public-Private Ventures (PPV), and similar programs designed to make the Department more efficient, ensuring that both CIP and the efficiency program can be implemented effectively.

e. The Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN(M&RA)) shall:

(1) Serve as a member of the DON CIP Council;

(2) Provide the DON Personnel Sector lead to the DON CIP Working Group, who will also serve as the DON representative to the OSD(P&R)-led OSD CIP Personnel sector working group;

(3) Identify and rank critical, DON owned and managed, personnel management infrastructures; and

(4) Participate in the conduct of vulnerability assessments of DON critical personnel infrastructures and develop CIP sensitive procedures for remediation, mitigation, and assurance that the minimum essential level of financial operations can be protected and maintained.

f. The Director, Naval Criminal Investigative Service (NAVCRIMINVSERV) shall:

(1) Serve as a member of the DON CIP Council, and provide a representative(s) to the DON CIP Working Group in the areas of Assessment and Indications and Warning (I&W);

(2) In partnership with the Office of Naval Intelligence (ONI), coordinate with DON CIAO in developing a comprehensive Indications and Warning capability of threats to Critical Infrastructures from unconventional sources (i.e., Foreign Intelligence Services, terrorism, etc.);

(3) Participate in the development and execution of an expanded NIVA process;

(4) Assist in identifying CIP weaknesses and vulnerabilities and in the development of strategies for remediating same; and

(5) Continue to lead and sponsor CNO (N34) Integrated Vulnerability Assessments.

g. The Office of General Counsel (OGC) shall serve as a member of the DON CIP Council and provide legal counsel in support of CIP efforts.

h. The CNO and CMC shall:

(1) Be responsible for the Critical Infrastructure Protection Program and attendant directions within their respective services;

(2) Contribute leadership on the DON CIP Council per enclosure (2);

(3) Provide sector action officers to the DON CIP Working Group per enclosure (3), and who will also serve as DON representative(s) to their respective OSD/Defense Agency CIP sector working groups;

(4) Implement DON CIP policy for the Navy and Marine Corps, respectively;

(5) Advise the DON CIAO on policy recommendations for CIP;

(6) Incorporate CIP into appropriate training programs;

(7) Work with the DON CIAO and the DON CIP Council to ensure that identified vulnerabilities to critical

infrastructures are given appropriate consideration in planning, programming, budgeting, and operations;

(8) In addition to the above, CNO shall assign the Joint Program Office for Special Technology Countermeasures to participate in the development and execution of an expanded NIVA process and further contribute its specialized skills and CIP-related products at the request, and under the direction, of the DON CIAO;

(9) Ensure every command and unit formally appoints a CIP point of contact;

(10) Assess vulnerabilities to critical systems and assets within their area of responsibility using provided self-assessment tools or the NIVA process;

(11) Establish a risk management plan to determine the maximum level of acceptable risk to identified critical infrastructures, based on their contribution to war fighting mission and system vulnerability;

(12) Coordinate with appropriate unified or specified commander(s), as well as applicable DoD and DON Infrastructure Sector managers, the prioritization of critical infrastructure vulnerabilities and remediate their risk, as appropriate in the event an installation or claimant is identified as a Joint Chiefs of Staff (JCS), CINC, or DoD Tier 1 or Tier 2 asset. Except for measures clearly peculiar to a tenant's mission, the host shall exercise general authority over tenants for coordination of CIP issues; and

(13) Develop and submit, to higher authority, when requested, for host installations and tenant commands, local plans for CIP remediation and mitigation, CIP tabletop and actual exercises, and local CIP best practices.

Gordon R. England

Distribution:
SNDL A1A (SECNAV)
A1B (UNSECNAV)
A1F (ASSTSECNAV FMC)

Distribution: (Cont'd)

| | |
|---|---|
| A1G | (ASSTSECNAV IE) |
| A1H | (ASSTSECNAV MRA) |
| A1J | (ASSTSECNAV RDA) |
| A1K | (OGC) |
| A2A | (DON Staff Offices (AUDGEN, CNR, DON CIO, JAG, OLA, NAVINSGEN, OPA, DONPIC, NAVCRIMINVSERV only)) |
| A3 | (Chief of Naval Operations) |
| A6 | (CMC) |
| 41A | (COMSC) |
| FE2 | (FLTINFOWARCEN) |
| FF42 | (NAVPGSCOL) |
| FF44 | (NAVWARCOL) |
| FKA1A | (COMNAVAIRSYSCOM) |
| FKA1B | (COMSPAWARSYSCOM) |
| FKA1C | (COMNAVFACENGCOM) |
| FKA1F | (COMNAVSUPSYSCOM) |
| FKA1G | (COMNAVSEASYSCOM) |
| FN1 | (COMNAVSPACECOM) |
| V28 | (CDR MARCORSYSCOM) |
| OPNAV | ((N09B, N1, N2, N3/N5, N4, N6, N7, N8, N091, N093, N095, N096, N00N)) |

Copy to:

| | |
|---|---|
| SNDL 21A | (FLEET CINCs) |

# Glossary of Department of the Navy Critical Infrastructure Protection Terms

**Assessment (CIP).** (1) An assessment is an objective evaluation of the vulnerabilities associated with Joint Force Capabilities. (2) Objective determination of how critical the capability and supporting infrastructure is in supporting military operations that accomplish the National Military Strategy. Focus is Combatant Command OPLANs. (3) A process to characterize the Department of Defense (DoD) infrastructures, their dependencies and interdependencies and subsequent linkages to commercial, foreign and host nation infrastructures.

**Asset.** Any military/private/commercial resource, relationship, instrument, installation, supply or system that in some combination is used in a military operational or support role. Assets are found at CONUS and OCONUS locations.

**Asset Criticality.** Measure of impact of asset that supports other assets, infrastructures, or operational plans.

**Assurance (Critical Capability/Infrastructure).** Assurance is guarding against the loss or disruption of a critical capability/infrastructure. Assurance assumes the identification of capabilities, assets, nodes, and infrastructures deemed critical to the Department of Defense in peacetime, crisis and war. Assurance requires assessing potential threats and identifying potential actions to restore those capabilities, assets, nodes, and infrastructures (or functionality they provide) if they are lost, damaged, corrupted, or compromised. Further, assurance requires identifying and resourcing options to protect, mitigate, and improve the availability of these Critical Capabilities and Infrastructures that DoD organizations own, use, and control.

The goal of assurance is to inform planners and decision makers of the probability of availability and quality (e.g., integrity, reliability, confidentiality, survivability, endurability, capacity, adequacy) of specific capabilities and infrastructures. Examples of assurance activities are dedication of physical protection resources, development of redundant capability/means, alter OPLANS and CONPLANS that depend on the identified capability or accept risk and do

nothing. Assurance of a Critical Capability and/or Infrastructure is a shared responsibility. (DoDD 5160.54) (DoD CIP Plan of November 1998)

**Asymmetric Warfare.** The attempts to circumvent or undermine a nation's strengths while exploiting its weaknesses by using methods other than conventional warfare, such as: terrorism, (physical and cyber), information warfare, space warfare, and weapons of mass destruction.

**Capability (Threat).** The ability of a suitably organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communication systems and/or to disrupt, deny or destroy all or part of a critical infrastructure. Increased asymmetric threat activity indicates a patchwork of actors that may not individually possess the capability to affect critical capabilities or infrastructures but collectively in loose alliances have increase ability and intent. (National Plan (NP) V 1.0)

**Capability (CINC/Joint Force). Military Capability:** The ability to achieve a specific wartime objective (win a war or battle, destroy a target set). It includes four major components: force structure, modernization, readiness, and sustainability.

(a) **Force structure.** Numbers, size, and composition of the units that comprise our Defense forces; e.g., divisions, ships, airwings.

(b) **Modernization**. Technical sophistication of forces, units weapons systems, and equipment.

(c) **Unit Readiness**. The ability to provide capabilities required by the combatant commanders to execute their assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed.

(d) **Sustainability.** The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materials, and consumables necessary to support military effort.

**Computer Emergency Response Team (CERT).** An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems. (DoDD 5160.54) (NP V 1.0)

**Critical Asset/Critical Node/Critical Item (Critical Infrastructure).** (1) Asset which can be either a DoD or non-DoD military-related unit, organization, facility/installation, system, resource, equipment, instrument, which is identified as performing an essential service, function, or use in military operational plans or support to operational plans. (2) Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical Assets may be DoD assets or other government or private assets, domestic or foreign, whose disruption or loss would render DoD Critical Assets ineffective or otherwise seriously disrupt DoD operations. Critical Assets include both traditional “physical” facilities or equipment, non-physical assets (such as software systems) or “assets” that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

- **Critical Node.** An element position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control or effectively conduct combat operations.

- **Critical Item.** An essential item which is in short supply or expected to be in short supply for an extended period. (Joint Publication (JP) 1-02)

**Critical Infrastructure.** Those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DoDD 8500.1 (NOTAL))

**Critical Infrastructure Assurance Officer (CIAO).** The CIAO is responsible for the protection of all of the department’s

critical infrastructures. The CIAO shall establish procedures for obtaining expedient and valid authority to allow vulnerability assessments to be performed on computer and physical systems. The Department of the Navy CIAO is the Department of the Navy Chief Information Officer, who was initially appointed by Under Secretary of the Navy memorandum of 26 August 1999 (NOTAL). The DON CIAO chairs the DON Critical Infrastructure Protection Council.

**Critical Infrastructure Protection (CIP).** CIP is Mission Protection. CIP is the identification, assessment, and assurance of Cyber and Physical infrastructures that support mission critical capabilities and requirements, to include the political, economic, technological, and informational security environments essential to the execution of the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DoDD 8500.1(NOTAL))

**Critical Infrastructure Protection Council.** The Department of the Navy Critical Infrastructure Protection Council: (a) determines the necessary efforts to institute Critical Infrastructure Protection throughout the DON; (b) contributes subject matter experts to support OSD sector CIAOs; (c) identifies resource sponsors and asset owners responsible for DON critical infrastructures; and recommends resource actions to support implementation.

**Criticality Index, Criticality Metric.** Measurement established within an asset class, organization or sector, to assist in ranking assets for assurance or protection activities. An example would be a graduated indicator of impact from system-wide slight degradation of service to cessation of operations. (Department of Defense Critical Asset Assurance Program Working Definition)

**Criticality-Vulnerability Ratio.** Comparison of criticality and vulnerability indices. (Department of Defense Critical Asset Assurance Program Working Definition)

**Defense Critical Infrastructure.** Those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degredation jeopardize the ability of the DoD to execute the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DoDD 8500.1(NOTAL))

**Defense Information Infrastructure.** The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DoD local, national and worldwide information needs. The Defense Information Infrastructure connects DoD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information and is also called DII. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Publication 1-02)

**Defense Infrastructure.** Infrastructure owned, operated or provided by the Department of Defense. Defense Infrastructure Sectors include the Defense Information Infrastructure (DII), Command/Control/Communications (C3), Space, Intelligence/ Surveillance/Reconnaissance (ISR), Financial Services, Logistics, Public Works (includes DoD owned or operated utilities, roads, rails and railheads and their interface to commercial and other Government systems), Personnel, Health Affairs and Emergency Preparedness. (See also definitions of Infrastructure, National Infrastructure, National Defense Infrastructure, and International Defense Infrastructure.)

**Denial of Service.** A form of attack that reduces the availability of a resource. (NP V 1.0)

**Destruction.** A Condition when the ability of a critical infrastructure to provide its customers an expected level of products and services is negated. Typically a permanent condition. An infrastructure is considered destroyed when its level of performance is zero. (NP V 1.0)

**DoD Installation.** A facility subject to the custody, jurisdiction, or administration of any DoD Component. This term includes, but is not limited to, military reservations, installations, bases, posts, camps, stations, arsenals, or laboratories where a DoD Component has operational responsibility for facility security and defense. Examples are facilities where the military commander or other specified DoD

official under provisions of DoD Directive 5200.8 of 25 April 1991, has issued orders or regulations for protection and security. Both industrial assets and infrastructure assets, not owned by the Department of Defense, may exist within the boundaries of a military installation (DoDD 5160.54)

**Force Protection.** Security program designed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

**Global Information Infrastructure.** The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The Global Information Infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of JP 1-02)

**Guidance.** (1)Policy, direction, decision, or instruction having the effect of an order when issued by a higher echelon. (2) The entire process by which target intelligence information received by the guided missile is used to effect proper flight control to cause timely direction changes for effective target interception. (JP 1-02)

**Incapacitation.** An abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact. (NP V 1.0)

**Indications and Warning.** Indications are preparatory actions or preliminary infrastructure states that signify that an incident is likely, is planned, or is underway. An official warning would be issued by the responsible organization.

**Information Assurance.** (1) Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities and is also called IA. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02) (2) Information operations that protect key public and private elements of the national information infrastructure from exploitation, degradation, and denial of service. (Modified from NSTAC)

**Information Operations.** Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

**Information Security.** Information Security is the protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information Security includes the measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

**Information Superiority.** The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02)

**Information System.** The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

**Infrastructure.** The framework of inter-dependent networks and systems comprising identifiable industries, institutions, functions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole. (DoDD 5160.54) (DoD Plan – November 1998) (NP V 1.0) Bilateral Infrastructure – page 58 JP 1-02, Common Infrastructure – page 93 JP 1-02, National Infrastructure – page 302 JP 1-02.

**Infrastructure Analysis and Assessment.** Coordinated identification of DoD, National Defense Infrastructure, and International Defense Infrastructure critical assets, their system and infrastructure configuration and characteristics, and the interrelationships among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets/ infrastructures; and assessment of the operational impact of loss or compromise. (CIP Working Definition) (DoD Plan – November 1998)

**Infrastructure Asset.** Any infrastructure facility, equipment, service or resource that supports a DoD Component. A Critical Infrastructure Asset is an infrastructure asset deemed essential to DoD operations or the functioning of a Critical Asset. (DoDD 5160.54) (DoD Plan – November 1998)

**Infrastructure Assurance.** Planning to improve the readiness, reliability, and continuity of infrastructures such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in event of disruption or attack; and (3) can be readily reconstituted to reestablish vital capabilities. It includes those efforts that protect infrastructures, assure their readiness, reliability, and continuity of infrastructures such that they are: less vulnerable to disruptions or attack,

harmed to a lesser degree in the event of a disruption or attack, and can be readily reconstituted to reestablish vital capabilities. (DoD CIP Plan) Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage, e.g., incident mitigation, incident response, and service restoration. (NP V 1.0)

**Infrastructure Indications and Warning.** Tactical indications through the implementation of sector monitoring and reporting, strategic indications through Intelligence Community support, and warning in coordination with the National Infrastructure Protection Center (NIPC) in concert with existing DoD and national capabilities. (CIP Working Definition)(DoD Plan – November 1998)

**Infrastructure Protection.** Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures. For instance, threat deterrence and vulnerability defense.

**Interdependability.** Dependability between elements or sites of different infrastructures, and therefore, effects of one infrastructure upon another.

**Interdependence.** Dependence among elements or sites of different infrastructures, and therefore, effects of one infrastructure upon another. (DoD Plan – November 1998) (NP V 1.0)

**International Defense Infrastructure.** Those elements of international infrastructure that are critical to Department of Defense operations. (CIP Working Definition) (DoD Plan – November 1998)

**Metrics.** An agreed-upon measure of performance. (NP V 1.0)

**Military Capability.** See "Capability"

**Military Requirement.** An established need justifying the timely allocation of resources to achieve a capability to accomplish approved military objectives, missions, or tasks. Also called operational requirement. (JP 1-02)

**Military Strategy.** The art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force or the threat of force. See also Strategy. (JP 1-02, p. 287)

**Mission Critical.** Systems handling information which is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). (NP V 1.0)

**Mission Essential.** Any asset or function that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

**Mitigation.** Action taken to reduce or eliminate vulnerability of people or infrastructure to threats and their effects. (Joint Staff Definition used in coordinated response to Draft DoDD 8500.1 (NOTAL))

**National Defense Infrastructure.** Those assets in the other government and national infrastructure sectors and industrial assets that are critical to National Defense. (CIP Working Definition)(DoD Plan – November 1998)

**National Infrastructure.** Those infrastructures essential to the functioning of the nation and whose incapacity or destruction would have a debilitating regional or national impact. National infrastructures include telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation, emergency services, and continuity of government operations. (DoDD 5160.54) (DoD Plan – November 1998)

**National Information Infrastructure.** The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The National Information Infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire,

satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. Also called NII. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition modifies the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

**National Military Strategy.** The art and science of distributing and applying military power to attain national objectives in peace and war. See also Military Strategy; National Security Strategy; Strategy; Theater Strategy. (JP 1-02, p. 302)

**National Security Strategy.** The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives which contribute to national security. Also called national strategy or grand strategy. See also Military Strategy; National Military Strategy; Strategy; Theater Strategy. (JP 1-02, p. 303)

**National Strategy.** The art and science of developing and using political, economic, and psychological powers of a nation, together with its armed forces, during peace and war, to secure national objectives. See also strategy. (JP 1-02, p. 303)

**Naval Integrated Vulnerability Assessment.** An expert third party or peer review comprehensive CIP assessment instrument under DON CIAO coordination and leadership synthesizing several existing assessment protocols including Marine Corps or CNO Integrated Vulnerability Assessments for Anti-terrorism and Force Protection; Marine Corps Enterprise Network (MCEN) or Fleet Information Warfare Center (FIWC) assessments for computer network vulnerability; non-organic and other commercial infrastructure assessments performed by Joint Program Office – Special Technology Countermeasures (JPO-STC) or other; and a continuity of operations plans and preparedness assessment under appropriate Navy or Marine Corps community direction. The NIVA is intended to be performed cyclically in all Navy Regions or other major Navy concentration areas, and at major Marine Corps Installations.

**Network.** Information system implemented with a collection of interconnected nodes. (NP V 1.0)

**Operational Impact.** Impact of critical assets and OPLANS on other military operations (mobilization, deployment, force projections, etc.)

**Operational Impact Analysis.** The relationship between military plans and operations and critical assets established through the development of operational dependency matrices and application of operations research methodologies.

**Operations Security.** The process denying to potential adversaries information about capabilities and/or intentions by identifying, controlling and protecting generally unclassified evidence of the planning and execution of sensitive activities. (NIS)

**Physical Security**. (1) That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. See also Communications Security, Protective Security, Security. (JP 1-02, page 343) (2) Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks, e.g., through the use of conventional or unconventional weapons. (NP V 1.0)

**Presidential Decision Direction/NSC-63.** The statement of National intent to protect infrastructures, both cyber and physical, deemed critical to sustainment of the American way of life.

**Public Key Infrastructure.** Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (NP V 1.0)

**Reconstitution.** Refers to actions required to rebuild or restore an aspect or portion of an infrastructure after it has been degraded. Owner/operator directed restoration of critical assets and/or infrastructure. (DoD Plan – November 1998)

**Red Team.** Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems. (NP V 1.0)

**Reliability**. The capability of a computer, or information or telecommunications system to perform consistently and precisely, according to its specifications and design requirements, and to do so with high confidence. (NP V 1.0)

**Remediation.** Those precautionary actions taken before undesirable events occur to improve known deficiencies and weaknesses that could cause an outage or compromise a defense infrastructure sector or critical asset. Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc., of critical assets and/or infrastructures, e.g., emergency planning for load shedding, graceful degradation, and priority restoration; increased awareness, training, and education; changes in business practices or operating procedures, asset hardening or design improvements, and system-level changes such as physical diversity, deception, redundancy, and back-ups. (NP V 1.0) (CIP Working Definition). (DoD Plan – November 1998)

**Response.** Response refers to those activities undertaken to eliminate the cause or source of an event. It also includes emergency measures from dedicated third parties such as medical, police, and fire and rescue (Public Safety). Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident. (NP V 1.0)

**Risk.** The probability that a particular threat will exploit a particular vulnerability of the system (NSA, NCSC Glossary October 1988). The probability of a particular critical infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation. (NP V 1.0)

**Risk Analysis or Risk Assessment.** The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk Analysis is part of Risk Management (NSA, NCSC Glossary October 1988) produced from the combination of Threat and Vulnerability Assessments characterized by analyzing the probability of destruction or

incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities. (NP V 1.0)

**Risk Management.** The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review (NSA, NCSC Glossary, Oct 88). The deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level. Characterized by identifying, measuring and controlling risks to a level commensurate with an assigned value. (NP V 1.0)

**Scaling.** Ability to easily change in size or configuration to suit changing conditions. (NP V 1.0)

**Sector.** (1) One of two divisions of the economy (private or public); (2) A group of industries of infrastructures, which perform a similar function within a society, e.g. vital human services. (NP V 1.0)

**Sector Coordinator.** The majority of critical infrastructures are owned and operated by the private sector entities. Members of each critical infrastructure sector will designate an individual to work with the Federal Lead Agency Sector Liaison to address problems related to critical infrastructure protection and recommend components for the National Plan for Information Systems Protection. (NP V 1.0)

**Sector Liaison.** An individual of Assistant Secretary rank or higher designated by each Federal Lead Agency who cooperates with private sector representatives in addressing problems related to critical infrastructure protection and recommending components for the National Plan for Information Systems Protection. (NP V 1.0)

**Sector Coordinator Responsibilities.** Identification of the sector's critical assets and system-level characterization of the sector. Others in DoD CIP Plan Draft.

**Shared Risk.** Refers to risk that, when accepted at a single Department Activity, subjects all users of interconnected systems and networks to the same risk.

**Strategy.** The art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lesson the chances of defeat. See also Military Strategy; National Strategy. (JP 1-02, pages 429-430)

**Threat.** A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and malicious intent of debilitating the defense or economic security of the United States. A threat may be an individual, organization, or nation. (NP V 1.0)

**Threat Analysis.** A continual process of compiling and examining all available information concerning potential conventional and asymmetric force activities by groups which would target a asset, facility, node, capability, or infrastructure. A threat analysis will review the factors of a hostile groups' existence, capability, intentions, history and targeting as well as the security environment within which the friendly forces operate. Threat analysis is an essential step in identifying probability of conventional/asymmetric attack and results in a threat assessment.

**Tier Definitions.** As determined by the geographic Commanders in Chief:

- Tier I - Warfighter suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.

- Tier II - Sector or element suffers strategic functional failure, but warfighter strategic mission is accomplished.

- Tier III - Individual element failures, but no debilitating strategic mission or core function impacts occur.

- Tier IV - Everything else.

**Vulnerability.** (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight

diminished. (2) The characteristics of a system which cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in a unnatural (manmade) hostile environment. (3) In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition replace the existing term and its definition and are approved for inclusion in the next edition of Joint Pub 1-02.) A characteristic of a critical infrastructure design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat. (NP V 1.0)

**Vulnerability Assessment.** Assessment of probability that events will occur using scenario-driven vulnerability index. Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation. (NP V 1.0)

**Vulnerability Metrics.** The modeling of actual data supporting vulnerability ratios and indices onto a matrix frame work that will show relationships and dependencies of mission, task, function and infrastructure. (JPO-STC)

**DEPARTMENT OF THE NAVY**
**CRITICAL INFRASTRUCTURE PROTECTION COUNCIL**

Under Secretary of the Navy

DON CIAO

Deputy DON CIO for E-business and Security (Deputy CIAO)

Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RDA))

Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN (FM&C))

Assistant Secretary of the Navy (Installations and Environment) (ASN (I&E))

Assistant Secretary of the Navy (Manpower & Reserve Affairs) (ASN (M&RA))

Director, Office of Program Appraisal (OPA)

General Counsel (OGC)

Director, Naval Criminal Investigative Service (NAVCRIMINVSERV)

Assistant for Special Programs and Intelligence, Office of the Under Secretary of the Navy (OUSN (ASP/I))

Surgeon General of the Navy (N093)

Director of Naval Intelligence (N2)

Deputy Chief of Naval Operations (Plans, Policy & Operations) (N3/5)

Director, Anti-Terrorism/Force Protection Division (N34)

Deputy Chief of Naval Operations (Fleet Readiness & Logistics) (N4)

Director, Space Information Warfare Command & Control (N6)

Deputy Chief of Naval Operations (Naval Warfare)(N7)

Deputy Chief of Naval Operations (Resources, Warfare Requirements & Assessments) (N8)

Deputy Commandant, Plans Policies & Operations (USMC PP&O)

Commander, Military Sealift Command (MSC)

The DON CIP Council shall:

1. Convene as directed by the DON CIAO;

2. Determine the necessary efforts to institute CIP efforts throughout the Department of the Navy;

3. Contribute Subject Matter Experts to support OSD sector CIAOs;

4. Identify resource sponsors and asset owners responsible for DON critical infrastructures, and

5. Recommend resource actions to support implementation.

**DEPARTMENT OF THE NAVY**
**CRITICAL INRASTRUCTURE PROTECTION**
**WORKING GROUP**

| SECTOR | LEAD(S) NAVY/MARINE CORPS |
|---|---|
| Chair | - DON CIO Special Assistant for CIP |
| Indications & Warnings | - Anti-Terrorism/Force Protection (N34)<br>- Naval Criminal Investigative Service<br>- Office of Naval Intelligence |
| Assessments | - Joint Project Office for Special Technology Countermeasures<br>- Naval Criminal Investigative Service |
| Personnel | - Bureau of Naval Personnel<br>- USMC Manpower |
| Health Affairs | - Director Medical Resources, Plans & Policy Division (N931) |
| Financial Services | - Director of Financial Operations (FMO) |
| Logistics | - Director of Supply Programs & Policy Division (N41)<br>- War Reserve Materiel & Readiness Branch (HQMC I&L (LPP-1)) |
| Transportation | - Director of Supply Programs & Policy Division (N41) |
| Space | - Space Systems Division (N63) |
| Defense Information Infrastructure/Command, Control, Communications | - Information Warfare Division (N64)<br>- Deputy Assistant Chief of Staff for Systems Integration (HQMC (C4)) |
| Intelligence, Surveillance, and Reconnaissance | - Director, Requirements, Plans, Policy Programs Division (N20) |

| | |
|---|---|
| Public Works | - Director, Ashore Readiness Division (N46)<br>- Director, Facilities & Services Division (HQMC I&L (LF)) |

The DON CIP Working Group shall:

1. Meet as needed in support of continuing CIP developments. Report progress to, and receive direction from, the DON CIP Council;

2. Interface directly with the DoD CIPIS providing expertise and input on the development of CIP products;

3. Provide input to support future CIP policy, and

4. Assist CINCs and regional asset owners as needed in identifying critical infrastructures to be assessed in existing and future IVA processes.